Mouse Jigglers Zero Trust Hardware Access

Trust does not end at secured login

The Challenge

Mouse jigglers are designed to simulate user activity and keep systems from locking or appearing idle. Whether introduced as a small USB peripheral or another unmanaged input device, they create a policy gap: the user may be legitimate, but the connected hardware is not. That blind spot undermines Zero Trust, insider-risk controls, remote-work policies, and physical security assumptions.

Why It Matters Now

As organizations tighten identity, MFA, and application controls, attackers and insiders look for simpler ways to bypass the spirit of those protections. A mouse jiggler can help defeat inactivity-based safeguards, mask unauthorized presence, and keep a trusted session alive longer than intended. Security teams need to verify the device itself-not just the user behind it.

Sepio's Solution

Sepio brings Zero Trust to the hardware layer. Using physical-layer intelligence and AssetDNA-based identification, Sepio can discover and classify connected peripherals, verify their true hardware identity, and detect unauthorized or non-compliant devices even when they try to appear as ordinary human-interface equipment. That allows organizations to enforce hardware access policy based on evidence, not assumption.

How Sepio Addresses the Mouse Jiggler Challenge

Sepio supports the five operational pillars of Zero Trust Hardware Access:

1

Discover

Gain visibility into connected USB and endpoint peripherals, including devices that traditional EDR, XDR, or policy controls may overlook.

2

Verify Identity

Establish the true hardware identity of the connected device using physical-layer characteristics rather than trusting the device's declared type alone.

3

Validate Posture

Continuously assess whether the peripheral belongs in that role, on that endpoint, for that host, and under that policy context.

4

Prioritize Risk

Elevate suspicious or unauthorized devices based on business context, user sensitivity, exposure, and operational urgency.

5

Enforce and Mitigate

Trigger alerts, block ports, isolate endpoints through integrated controls, or launch automated workflows before the device can support policy evasion.

Why Sepio

- See unmanaged peripherals and suspicious input devices that may be invisible to identity- or application-centric controls
- Verify device identity using AssetDNA and physical-layer characteristics
- Detect unauthorized USB human-interface devices in real time
- Enforce granular hardware access policies for endpoints, users, and locations
- Integrate with existing security operations to accelerate mitigation and response.

Sepio strengthens Zero Trust by making hardware trust verifiable. For the mouse jiggler problem, that means security teams are not limited to judging the session or user alone-they can also verify whether the connected hardware is authorized, expected, and appropriate for that environment.

Business Outcomes

- Reduce exposure from policy-evasion tools such as mouse jigglers and rogue peripherals
- Strengthen Zero Trust by extending verification to the hardware layer
- Improve compliance with remote-work, session-control, and endpoint-use policies
- Support faster, more accurate investigations with evidence-based device identity
- Increase defender confidence that trusted sessions are not being propped up by untrusted hardware.

A trusted user should not be able to rely on an untrusted device

Sepio helps organizations extend Zero Trust to the physical layer-so policy-evasion tools like mouse jigglers can be discovered, verified, and stopped before they undermine control.